




Seminar 4

Security Standards

Team 3

Jonathan Ashmore



Which of the standards discussed in the sources above would apply to the website/ organisation assigned to you for the assessment?

- Evaluate your assigned website against the appropriate standards and decide how you would check if standards were being met?
- What would your recommendations be to meet those standards?
- What assumptions have you made?

Questions





Introduction

- Our assigned website is a Customer Relationship Management(CRM).
- CRM is a set of ideas and principles that helps businesses engage and connect with customers and their data. Organisations are moving their customers' data to the cloud and using CRM platforms such as Salesforce, and Dynamics 365 (Martin, 2010).

Which of the standards discussed in the sources above would apply to the website/ organisation assigned to you for the assessment?

GDPR

PCI-DSS

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) which comes under the UK GDPR standard of consent.

Others include ISO 27000, DPA 2018, GDPR 2016

Evaluate your assigned website against the appropriate standards and decide how you would check if standards were being met?

External auditors and consultants to verify compliance.

GPDR:

Security including pseudonymization, encryption. Ensure Confidentiality, Integrity, and Availability (CIA), fairness of data usage; minimise data it is adequate, relevant, and necessary. Accountability and responsibility of personal data, and compliance with relevant regulations.

PCI-DSS:

PIN Transaction security point of interaction, Payment Application Data Security Standard, PTS Hardware Security model, P2PE, PCI 3-D Secure Software Development Kit; Software-based PIN Entry on COTS, Secure Software, Contactless Payments on COTS

What would your recommendations be to meet those standards?

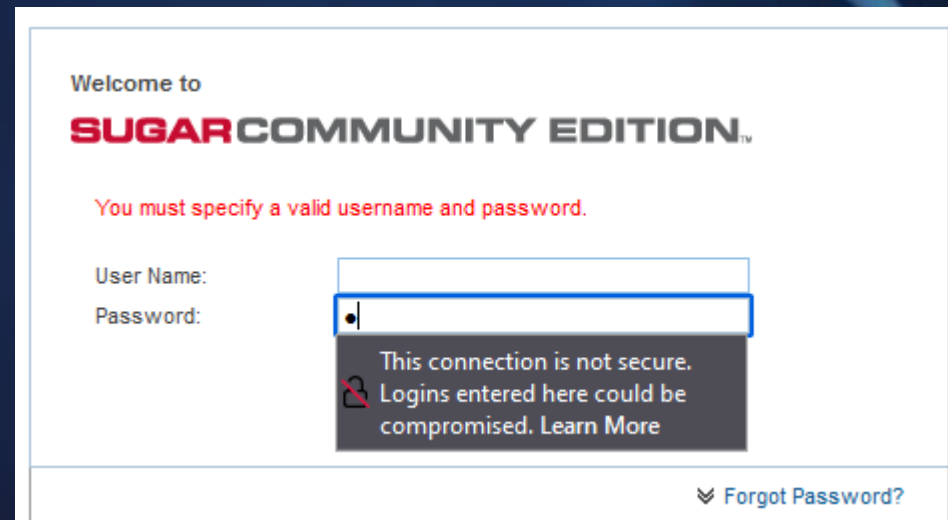
Information Commissioner's Office recommends the following:

- consider things like risk analysis, organisational policies, and physical and technical measures.
- take into account additional requirements about the security of your processing – and these also apply to data processors.
- You also need to ensure that you have appropriate processes in place to test the effectiveness of your measures, and undertake any required improvements.
- Set up a committee, determine budget, costs, and timeframe- Action plan

What assumptions have you made?

www.customersrus.co.uk is an old website with outdated software and vulnerabilities. Firefox browser flags the password input box. GDPR stipulates 'Any password system you deploy must protect against theft of stored passwords and 'brute-force' or guessing attacks.'

Also, there is no cookie notification which contravenes UK GDPR standard of consent.



Welcome to
SUGAR COMMUNITY EDITION™

You must specify a valid username and password.

User Name:

Password:

This connection is not secure.
Logins entered here could be compromised. [Learn More](#)

[Forgot Password?](#)

References

- CookieFirst - Cookie Consent Management. (2022) *Cookie notice*. Available from: <https://cookiefirst.com/cookie-notice/#:~:text=A%20cookie%20notice%20is%20the%20banner%20that%20appears> [Accessed 27 Apr. 2022].
- Ico.org.uk. (2019) *Passwords in online services*. Available from: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/passwords-in-online-services/> [Accessed 27 Apr. 2022].
- ico.org.uk. (2022) *What are PECR?* Available from: <https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/#:~:text=The%20e-privacy%20Directive%20complements%20the%20general%20data%20protection> [Accessed 27 Apr. 2022].
- Ico.org.uk.(2019) *Guide to the General Data Protection Regulation (GDPR)*. ico.org.uk. Available from: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>.
- Pcisecuritystandards.org. (2019) *Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards*. Available from: https://www.pcisecuritystandards.org/pai_security/standards_overview [Accessed 27 Apr. 2022].
- Martin, J. (2010) Put Cloud CRM to Work. Available from: https://www.pcworld.com/article/511929/put_cloud_crm_to_work.html [Accessed 5 Apr. 2022].